Health Information Exchange
Privacy and Security Controls

Security and privacy are the core of the Health Information Exchange (HIE) and are integral parts of all functions that are conducted by CORHIO. CORHIO collaborates with communities and stakeholders to implement secure systems and processes for sharing clinical information. Our policies to protect the privacy and security of personal health information are developed and maintained by a statewide policy committee consisting of diverse representatives from across the Colorado healthcare community. A corner-stone of this committee is our shared commitment to privacy and security for all participants and patients in the CORHIO HIE.

Our statewide, hosted HIE infrastructure, platform, and services are provided by the joint partnership between CORHIO and Health Catalyst (formerly Medicity).

Certifications	CORHIO recently achieved HITRUST CSF® Certification, considered a gold standard in security oversight.
Data Center	• HIPAA and HITECH compliant data centers (primary and backup) • SOC 2 Type 2 • CORHIO-specific cages • 24/7/365 hosted system monitoring and full failover capabilities • Offsite backup storage
Software & Services	• Compliance with HIPAA and HITECH requirements for all services and deliverables • Annual Disaster Recovery/Business Continuity testing • Annual third party penetration testing and vulnerability scanning • Up time, response time, RPO/RTO SLAs to support 24/7 operations for critical incidents • Intrusion detection and prevention • Annual complete risk assessment • Center for Internet Security (CIS) Critical Security controls • Scheduled security updates
Data	Adhere to NIST guidelines for data encryption and backup media encryption
User Access	• Role-based access controls • Industry standard password strength and timeout requirements • User activities audited
Trained Workforce	• CORHIO workforce are trained and accountable for upholding state and federal laws, including HIPAA, HITECH and associated regulations, as well as all CORHIO policies and procedures. Additionally, the workforce is trained in cyber security incident response • CORHIO Security Response Team consists of a Compliance Officer, a Privacy Officer and a Security Officer
Support Procedures	CORHIO maintains robust internal and external user policies including but not limited to: appropriate use of services, maintaining authorized users, access auditing, inappropriate use and non-compliance reporting, system security safeguards, filtering sensitive data, breach investigation and notification.
Patient Choice (Opt Out)	Patients have the right to opt-out of having their information queried and viewed in the HIE. Clinical data for opted-out patients is not searchable or viewable in the community health record, even in the event of an emergency.

CORHIO
4500 Cherry Creek S Dr. Suite 820, Denver, CO 80246
www.CORHIO.org

Last updated 11/03/2021